~~EYES ONLY~~

31 August 1984

MEMORANDUM FOR: Director of Central Intelligence

FROM: Executive Director

SUBJECT: Trying to Solve the Leak Problem — a few ideas.

Others--most recently Eloise--have ably summarized all the ideas anyone has ever had on what is needed outside the Agency to help the whole USG deal with the leak question. My firm belief--widely shared I think--is that CIA is itself not a major source of leaks. My equally strong belief is that we will make more progress getting Government-wide steps to deal effectively with the leak issue if we first move aggressively to do all that is reasonably within our power to deal with the problem. Understanding then that most leaks undoubtedly occur elsewhere and by individuals not under our control, here are some things we might do to show that we are doing what we can to cope with the problem.

1. Mobilize our secretarial force to play an even greater, more positive, and more explicit role in managing the dissemination of intelligence product by components. The functions which might be considered include: doing draft distribution lists; regular calls to certain customers to see if products have been received and/or returned; keeping track of copies make; etc. Such an approach has certain obvious negative connotations, but it could also be seen, and presented positively--in the sense that it could represent an effort to provide better service to customers as well as to enhance the responsibilities of our secretarial workforce. Bringing off such a program would be difficult, but by no means impossible. Auditorium sessions about the special security responsibilities secretaries have and about the constructive and helpful role they especially can play in monitoring the dissemination of information would be a low cost and useful way to start; OTE might develop a program for our ongoing training effort.

2. Consider additional steps to raise our collective consciousness of security issues and to give high profile attention to our concerns. Here are three:

a) We might ask selected components to perform an information audit each year--accounting for all paper disseminated. If ten components did this each year, each Agency component would do one about every five years. An award might be given annually to the component which did the best job of managing the

~~EYES ONLY~~

CL BY Signer
DECL OADR

dissemination of its products. Most important: the very process of thinking about how to accomplish such an audit might ultimately have far reaching, useful effects on the way we disseminate our product.

b) Take steps to reduce the size and complexity of the resource management process, in an effort to apply more discipline to the sharing of programmatic information around the Community. Some believe that the Community and Agency budget processes, while greatly improved over ten years ago in many respects, may be conducted in such a way as to encourage too much discussion of some sensitive questions too widely, particularly on the Hill. Equally important, we may be encouraging our Committees to deal carelessly with compartmentation by our own example: Internal steps to tighten up our security practices significantly could have a useful spill-over effect on the Hill.

c) Consider whether we might find a way to reward component chiefs who are successful both at placing substantive product in the hands of those who need it and at managing the dissemination of their product so as to avert leaks. Over a five or ten year period an initiative of this type could--in addition to helping sensitize everyone to our problem--generate hundreds of practical suggestions for improvements in our techniques for disseminating intelligence.

3. Work towards the establishment of an Agency-wide system of "dissemination categories," each of which would represent a control system to contain specific intelligence information. Start with a category which would include only the most sensitive information. The rules for dealing with such intelligence might include: all documents in the category to be handcarried by a courier; no copies to be left behind; and no information to be shared with people not agreeable to being polygraphed on the topics within the category. Non-compliance with our explicit rules for this category would mean no more intelligence would be provided.

Additionally, the dissemination of information placed in this category might be the responsibility of a small group of security officers whose responsibilities would include:

- arrang~~ing~~e for physical handling or delivery of the information

X - coordinat~~ing~~e a customer list with the originator

- maintain~~ing~~ a record of who saw what, when

- arranging for occasional polygraphs of customers and others.

Even more revolutionary, how about developing a computer based system through which we would disseminate selected products? We would control and manage the system. This would allow us to provide (and control) access to selected current intelligence product from Headquarters. A dedicated mini computer, serving ~~perhaps 100~~ a limited number of senior customers, could be used to deliver spot reports, ~~the NID~~, and other products as appropriate. The system should be designed to eliminate the use of hard copy documents, access would be by password, people would only be sent products for which they were cleared, and a permanent "auditable" record of everyone having access to certain kinds of information would automatically be maintained.

A "dissemination category" approach such as this to the leak problem might enable us to:

- Develop a carefully controlled program designed to protect our most sensitive product.

- Help regenerate the political will to deal with the hard problem of controlling leaks by starting with a small (albeit important) group of customers, and by focussing on clearly sensitive intelligence from a "sources and methods" point of view.

- Sharply focus any investigation of leaks or intelligence within the system on a few individuals, thereby enhancing the chances for success.

- Start a meaningful program of a small enough scale to try to prevent a critical mass of opposition to our approach from forming before the program could prove its value.

- Communicate to all recipients of product in this category the fact that we are deadly serious about leaks.

Clearly such an approach could/should be implemented only after discussion with the President, because it would touch people all around him. I am aware of how difficult is has been historically for senior people to contemplate tough measures to deal with the leak situation. But isn't it conceivable that the implementation of such a tough-minded program would itself stop leaks of the material handled in the new system, avoiding the need to confront a senior person whom we suspect of poor security practices?

4. Finally, we might consider a system by which we would more formally designate kinds of customers and the type of intelligence they can receive based on an assessment of their security practices! This would obviously be a very

tricky business. But, managed adroitly and proceeding in a measured way, step by step, we might be able (over perhaps a five year period) to get outside acquiesence. Again, the key would be to find a narrow problem on which to start, with the intention that we would extend the appeal to other problems/issues over time. Such a program could eventually have profound implications. In addition to helping to solve the leak problem, it could mean for example, that we would ultimately need to play a much larger role in the clearance process for non-Agency people who see our products.

Two important caveats about these ideas or others like them: they should be sold internally as carefully as we should attempt to sell them externally. They probably won't work if they don't have widespread, active support in our building and in the Intelligence Community. Second, each is potentially a two-edged sword. To preclude other agencies misinterpreting our motives (and doing to us what they perceive we are doing to them) will take great care.

[redacted] 25X1

EYES ONLY

SECRET